REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested. Claims 23-24 and 32-33 are canceled, new claims 36-39 are added, and claims 1-22, 25-31, and 34-39 are pending in the application.

The withdrawn rejection of claims 1-35 under 35 USC §102(e) in view of U.S. Patent Publication No. 2003/0093563 to Young et al. is acknowledged with appreciation.

Claims 1 and 10 stand rejected under 35 USC §103 in view of U.S. Patent Publication 2003/0051130 by MeLampy et al. in view of U.S. Patent No. 6,795,920 to Bacha et al. This rejection is respectfully traversed, as the Examiner has failed to establish a prima facie case of obviousness.

Applicant traverses the Examiner's assertions that MeLampy discloses or suggests (e.g., in para. 27) the claimed establishment on an outbound interface of a ***plurality*** of IP- based secure connections with ***respective destinations*** based on receiving encrypted packets, let alone respective *streams* of encrypted packets, as claimed. In fact, para. 27 provides no disclosure or suggestion whatsoever of multiple secure connections, as claimed. Rather, para. 27 simply describes use of an encryption system for transferring data packets between media routers 118 and 136 via the Internet.

Further, para. 36 describes multiple *flows*, but does not provide any disclosure or suggestion of any ***secure connection***, as claimed. In fact, MeLampy provides no reference whatsoever to any type of secure ***connection*** with a destination.

In contrast, each of the independent claims specify establishing a plurality of IP-based ***secure connections*** with respective destinations. Each claimed secure connection is described in the specification as a "tunnel" (an encrypted tunnel) that is terminated by a destination endpoint (i.e., a tunnel endpoint); the secure connections are established by the outbound interface receiving encrypted packets generated by the cryptographic module according to IPSEC protocol.

Applicant further traverses the Examiner's assertions that MeLampy discloses or suggests the claimed ***reordering*** the corresponding group of the data packets (that is ***output to the cryptographic module***) according to a determined quality of service policy and the corresponding

assigned maximum output bandwidth. Rather, MeLampy describes in para. 33 that the traffic manager 206 is used simply for "measuring and enforcing IP session data flow rates", where "once a forwarding decision is made, the traffic manager 206 **queues the received packet into its respective IP flow and associated priority**.

Paragraph 34 (cited by the Examiner) also specifies that maximum data rates are enforced not by ***reordering*** the data packets, but by "either **dropping packets or marking them as eligible for discarding** if they are outside a bandwidth allocated for the data flow." (Para. 34, lines 5-7). Further, the multi-media router 118 may be instructed by a session router 116 to enforce an allocated bandwidth and bit rate, such that "if data is received at a higher bit rate than allowed by the session router, the data received at the higher bit rate is **not transmitted**" (para. 34, lines 10-12). As described above, para. 36 simply describes providing quality measurement on a per flow basis, but does not disclose or suggest ***reordering*** of the data packets, as claimed.

Applicant traverses the Examiner's assertion that para. 40 teaches the claimed reordering of data packets that are ***then output to the cryptographic module for generation of the encrypted packets***: the claims specify that the queuing module reorders the corresponding group of data packets, and that the corresponding queueing module outputs the data packets ***to the cryptographic module***. In contrast, para. 40 of MeLampy et al. describes the actual encryption technique of Fig. 4[1] that is applied to sequence numbers *in* the data packets, and not the claimed ***reordering*** of ***data packets*** that are then supplied to the cryptographic module:

> [0040] As shown by block 302, **sequence numbers** within the RTP flow are randomly shuffled. In accordance with the preferred embodiment of the invention, ***a sequence number is assigned to each RTP multi-media data flow packet*** within an RTP flow such that ***when an RTP multi-media data flow packet is received, the associated sequence number may be determined***. Randomization code is utilized to provide random shuffling of the sequence numbers. Preferably, the random shuffling is algorithmically predictable if a key to the randomization code is known. Therefore, since the randomly shuffled sequence numbers are algorithmically predictable if the key is known, the sequence

[1]"FIG. 4 is a flow chart illustrating operations performed by the present encryption system to provide encryption of multi-media data packets transmitted within RTP flows." (Para. 39, lines 1-4).

numbers really are not randomly shuffled but are instead, pseudo-randomly shuffled.

Hence, para. 40 describes that each encrypted packet includes a sequence number, and that the sequence numbers are "shuffled" (i.e., **randomized**) in step 302 to generate "pseudo-randomly shuffled" sequence numbers. Paragraphs 41-55 further illustrate "randomization of sequence numbers that are used to provide encryption of multi-media packets" (see para. 41, lines 2-4) by **replacing in step 302 an original sequence number with an encrypted sequence number**:

> [0055] Applying this mapping to the step of randomly shuffling sequence numbers within an RTP multi-media data flow (**block 302**), the first RTP multi-media data flow packet has a sequence number 1888747329 (which maps to 1), the second packet has a sequence number 1601588182 (which maps to 2), and so on. Using this algorithm, the receiving side may produce a sequence of expected sequence numbers and restore them. As an example, a sender that is transmitting an original sequence number of 1 (or a salt value of 1) may **replace the original sequence number with an encrypted sequence number** of 1888747329. The encrypted sequence number of 1888747329 may then be transmitted to a receiving side. Upon receipt of the encrypted sequence number, the side receiving may restore to the original sequence number of 1. Therefore, if the starting value, otherwise referred to as the original value, is known, an encrypted sequence number can be produced and decoded. However, if the original sequence number is not known, the encrypted sequence can not be anticipated and later decoded.

Hence, MeLampy does not disclose or suggest reordering the corresponding group of ***data packets***, as claimed.

Further, MeLampy teaches away from the claimed outputting ***to the cryptographic module*** the corresponding group of the data packets associated with the corresponding secure connection and reordered according to the determined quality of service policy and corresponding assigned maximum output bandwidth, enabling each encrypted packet output from the cryptographic module to have a "corresponding successively-unique sequence number". As demonstrated above, each of the sequence numbers are pseudo-randomly shuffled, and are no longer successively unique.

Moreover, MeLampy **explicitly teaches** that packets can be resequenced in step 306 **after**

the shuffling of sequence numbers in step 302 and encryption of data port addresses in step 304: [a]s shown by block 306, resequencing of the multi-media packets is **then performed** ..." (para. 60, lines 1-2); further, MeLampy **explicitly teaches** that "in accordance with the re-sequencing of multi-media data packets, the multi-media data packets may be transmitted **in any order desired**, including, but not limited to, 2, 5, 4, 1, 3, etc." (Para. 61, lines 7-10).

Hence, MeLampy teaches that the encrypted packets can be transmitted in any order desired; further, MeLampy fails to teach or suggest that the packets should be reordered and output ***to the cryptographic module*** according to the determined quality of service policy and based on the corresponding assigned output bandwidth; rather, MeLampy simply queues the packets for transmission, with no suggestion that the packets should be ordered ***prior to encryption***, as claimed.

Hence, MeLampy fails to disclose or suggest the claimed features, as asserted by the Examiner.

The Examiner also admits that MeLampy fails to disclose or suggest controlling supply of data packets to the cryptographic module by assigning, for each secure connection, a corresponding queuing module.

The Examiner's reliance on four lines of Bacha et al. (col. 9, lines 45-48) demonstrates an impermissible hindsight reconstruction, *especially* since Bacha is non-analogous art. Bacha et al. is directed to strong authentication of clients and servers using digital keys and digital certificates (see, e.g., col. 1, lines 39-45, col. 2, line 60 to col. 3, line 31), and is not within the field of the inventors' endeavor, namely "transport of Internet Protocol (IP) packets, requiring a guaranteed quality of service (QoS), via secure IP connections" (page 1, lines 2-3 of specification);[2] further, Bacha et al. is not reasonably pertinent to the particular problem with which the inventors were

---

[2]The Examiner is required to consider the disclosed specification in determining the appropriate field of endeavor: "[t]his test for analogous art requires the PTO to determine the appropriate field of endeavor by reference to explanations of the invention's subject matter in the patent application, including the embodiments, function, and structure of the claimed invention." *In re Bigio,* 72 USPQ2d 1209, 1212 (Fed. Cir. 2004) (citations omitted).

involved, namely preventing reordering of encrypted packets having sequence numbers to avoid dropping of out-of-order packets (see, e.g., page 3, line 5 to page 4, line 7 of specification). Bacha et al. provides no disclosure or suggestion of controlling supply of data packets ***to the cryptographic module*** by assigning, for each secure connection, a corresponding queuing module, and as such is non-analogous art. *In re Wood*, 202 USPQ 171, 174 (CCPA 1979). *In re Oetiker*, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992).

In fact, the disclosed feature in col. 9, lines 45-48 (claim 3), of "wherein the controller is further operative to maintain a queue with each secure area for use in storing and retrieving message information exchanged between different secure areas" is not a teaching of the claimed controlling supply of ***data packets to the cryptographic module*** by assigning, ***for each secure connection***, a corresponding queuing module. Rather, Bacha et al. describes with respect to Fig. 2 that each queue 203 is configured "for storing messages received **from other processes**"(see, e.g., col. 6, lines 32-34); further, Bacha et al. teaches that the queue 203 is used to receive **encrypted messages** output from the secure depositor 200 that performs the encryption:

> When a vault process running in vault 204^2 wants to send a message to vault 204^1, the Secure Depositor encrypts and signs the message **before inserting it into the queue 203^1 in vault 204^1**. If the process 202^1 happens to be running in vault and monitoring queue 203^1, the process will immediately receive the message. The process also uses its instance of the Secure Depositor to retrieve the message from its queue. The Secure Depositor decrypts the message and verifies the signature before returning the message content.
>
> (Col. 6, lines 44-47).

As apparent from the foregoing, the Examiner has failed to consider the teachings of Bacha et al. in its entirety, but instead applies a piecemeal approach by relying solely on **4 lines of the entire reference**. However, "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. MPEP §2141.02, page 2100-132 (Rev. 3, Aug. 2005) (*citing W.L. Gore & Assoc. v. Garlock, Inc.*, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984))(emphasis in original).

Hence, Bacha et al. does not disclose or suggest the claimed controlling supply of data packets ***to the cryptographic module*** by assigning, for each secure connection, a corresponding queuing module, as asserted by the Examiner.

Moreover, the Examiner has failed to demonstrate that one skilled in the art would have been motivated to modify MeLampy et al. to include the teachings of Bacha et al. in order to result in a hypothetical combination in the manner claimed. The Examiner is reminded that an obviousness rejection requires a specific showing as to why one of ordinary skill in the art would have selected the components for combination in the manner claimed.[3] "The examiner's conclusory statements ... do not adequately address the issue of motivation to combine. This factual question of motivation is material to patentability, and [cannot] be resolved on subjective belief and unknown authority. It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to '[use] that which the inventor taught against its teacher.'" *In re Lee,* 61 USPQ2d at 1434 (*quoting W.L. Gore v. Garlock, Inc.,*, 202 USPQ 303, 312-13 (Fed. Cir. 1983)).

The Examiner's argument of a motivation "to allow user processes running in dedicated vaults to communicate with other User [sic] processes running in different vaults" does not address the teachings of MeLampy et al. or the claimed supply of data packets (in a router) to a ***cryptographic module*** in the router ***for generation of the encrypted packets***. In fact, MeLampy describes encryption of multi-media **data flows**, which is well recognized as an Internet Protocol (OSI Network Layer 3) operation; in contrast, Bacha et al as non-analogous art is concerned with

---

[3]*Cf. In re Lee*, 61 USPQ2d 1430, 1433-34 (Fed. Cir. 2002) (*quoting In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 ("particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed"); *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1458 (Fed. Cir. 1998) ("the examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed." (emphasis added)).

authentication between **user processes** (OSI Application Layer 7)[4] between endpoint **host devices** by using personal storage vaults that store digital keys and digital certificates for authenticating the users (see, e.g., col. 1, line 53; col. 2, lines 3-4, 12-15, 23-29 and col. 2, line 61 to col. 3, line 37), and has no relevance whatsoever to the claimed transfer of ***encrypted packets*** via ***IP-based secure connections***. Hence, the supposed motivation to modify fails to address any motivation of modifying the media router of MeLampy et al. to control supply of data packets ***to the cryptographic module*** by assigning, for each secure connection (having a corresponding destination) a corresponding queuing module, as claimed.

In fact, the hypothetical combination fails to even address any desirability for any control in supplying data packets ***to the cryptographic module***. Hence, the unfounded assertions as to the teachings of MeLampy et al. and Bacha et al., plus the unfounded assertions of any motivation to modify the prior art to obtain a combination *in the manner claimed*, demonstrates an improper piecemeal analysis of the prior art that relies on the subject application as motivation to combine the references. "It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." *In re Fritch*, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992).

For these and other reasons, the §103 rejection of independent claims 1, 10, 18, and 27 should be withdrawn.

It is believed the dependent claims are allowable in view of the foregoing.

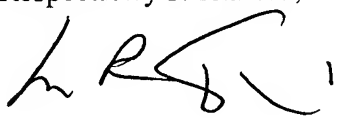
In view of the above, it is believed this application is in condition for allowance, and such a Notice is respectfully solicited.

---

[4]The attached Exhibit A demonstrates the distinctions between Application (Layer 7) operations as in Bacha et al., and Network (Layer 3) operations as in MeLampy et al.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R. 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a), to Deposit Account No. 50-1130, under Order No. 10-008, and please credit any excess fees to such deposit account.

Respectfully submitted,



Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
(202) 261-1059
Date: September 25, 2006

MENU
Home
Term of the Day
New Terms
Pronunciation
New Links
Quick Reference
Did You Know?
Categories
Tech Support
Webopedia Jobs
About Us
Link to Us
Advertising

Compare Prices
go
HardwareCentral

Talk To Us
Submit a URL
Suggest a Term
Report an Error

internet.com
Developer
International
Internet Lists
Internet News
Internet Resources
IT
Linux/Open Source
Personal Technology
Small Business
Windows Technology
xSP Resources
Search internet.com
Advertise
Corporate Info
Newsletters
Tech Jobs
E-mail Offers

internet commerce

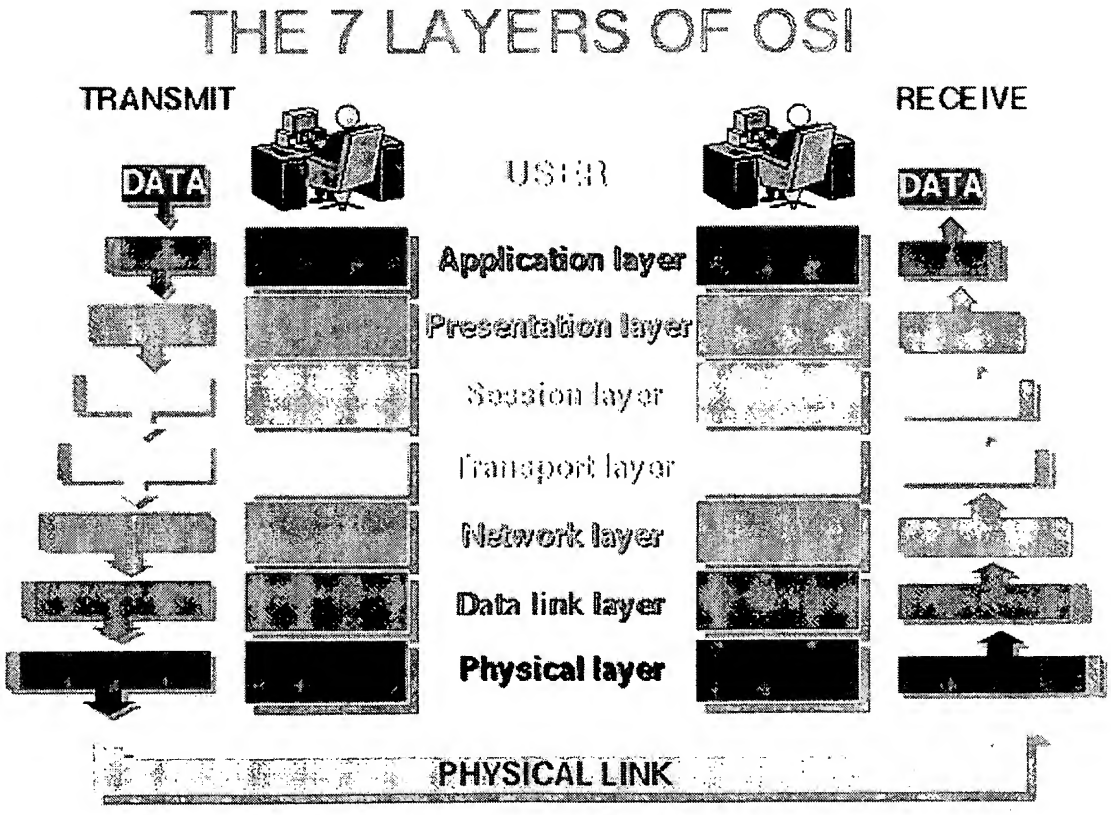
Home > Quick Reference

The 7 Layers of the OSI Model

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Application (Layer 7)	This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.
Presentation (Layer 6)	This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the *syntax layer*.
Session (Layer 5)	This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
Transport (Layer 4)	This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Network (Layer 3)	This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
Data Link (Layer 2)	At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
Physical (Layer 1)	This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.



This graphic is taken from The Abdus Salam International Centre for Theoretical Physics.